



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

| APPLICATION NO.   | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------|------------------|
| 09/957,415  | 09/20/2001  | Scott Thomas Elliott | RPS9 2001 0044      | 3264             |
| 47052   | 7590        | 12/13/2005           | EXAMINER            |                  |
| SAWYER LAW GROUP LLP<br>PO BOX 51418<br>PALO ALTO, CA 94303 |             |                      | CHAI, LONGBIT       |                  |
|   |             |                      | ART UNIT            | PAPER NUMBER     |
|   |             |                      | 2131                |                  |

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

|                              |                        |                     |  |
|------------------------------|------------------------|---------------------|--|
| <b>Office Action Summary</b> | <b>Application No.</b> | <b>Applicant(s)</b> |  |
|                              | 09/957,415             | ELLIOTT ET AL.      |  |
|                              | <b>Examiner</b>        | <b>Art Unit</b>     |  |
|                              | Longbit Chai           | 2131                |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 25 November 2005.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-22 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-22 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on 20 September 2001 is/are: a) accepted or b) objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) All    b) Some \* c) None of:
1. Certified copies of the priority documents have been received.
  2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)                     |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                    | Paper No(s)/Mail Date. _____  |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date. _____ | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
|   | 6) <input type="checkbox"/> Other: _____                                    |

**DETAILED ACTION**

1. This action is in response to the Appeal Brief filed on November 25, 2005. Claims 1 – 19 were originally received for consideration. Per the amendment received on May 13, 2005, new claims 20 – 22 were added and the claims 1 – 22 as pending in the application.

***Response to Arguments***

2. In view of the Appeal Brief filed on November 25, 2005, PROSECUTION IS HEREBY REOPENED. A new ground of rejection is set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

- (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,
- (2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 2, 9 and 17 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.

The claim limitation of claims 2, 9 and 17 “binding is required for the key pair material” is not enabled by the specification. According to the specification (Para [0020]), if the tag indicates that the key is a binding-required key, the embedded security chip only allows cryptographic functions to be performed using this key. If the tag indicates that the key is not designated as a binding required key, the embedded security chip allows all operations on the embedded security chip with that key regardless of binding. However, what constitutes all operations on the embedded security chip besides using only cryptographic functions to be performed is not specified and as such one skilled in the art clearly would not know how to make and use the same claimed invention to implement the case that the binding is required (or is not required) for the key pair material.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 5 and 13 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 5 and 13 are indefinite because the claim language "the four levels further comprise a hardware key pair level, a platform key pair level, a user key pair level, and a credential key pair level" is not consistently defined in the specification and is therefore not clear what the Applicant is exactly referred to. This is because, according to specification (Para [0019]), Level 0 is the hardware key pair, Level 1 is the platform key pair, Level 2 are a plurality of key encrypting key pairs and finally, Level 3 are user key pairs – instead of a hardware key pair, a platform key pair, a user key pair, and a credential key pair level for Level 0 – 3 respectively, as recited in claim 5 and 13, which is also presented in the specification (Para [0019]).

### **Claim Rejections - 35 USC § 103**

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A person shall be entitled to a patent unless –

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 7 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abgrall et al. (U.S. Patent 2003/0037237), in view of Bernstein et al. (U.S. Patent 2003/0012383).

As per claim 1, 7 and 16, Abgrall teaches a method for control of key pair usage in a computer system, the method comprising:

(a) creating key pair material for utilization with an embedded security chip of the computer system (Abgrall: Para [0191], [0105] and [0004] Line 16 – 19).

Abgrall teaches the key pair material is stored and bound to the embedded security chip. However, Abgrall does not disclose expressly the key pair material including tag data; and (b) determining whether the key pair material is bound to the embedded security chip based on the tag data.

Bernstein teaches the key pair material including tag data (Bernstein: Para [0005] and [0010]: Examiner notes key pair material is made with a reasonable and broadest interpretations and referred to as “any crypto-key related information that

enables the encryption / decryption functions" and Bernsteinet discloses "hardware footprint" as part of the decryption key (Bernsteinet: Para [0010] Line 6) that is interpreted as the "tag data" to meet the claim language).

determining whether the key pair material is bound to a specific computer based on the tag data (Bernsteinet: Para [0006] and [0005]: Examiner notes the digital content can only be successfully decrypted if the hardware blueprint contains the correct tag data associated with a specific machine (Bernsteinet: Para [0005]) and thereby, Examiner notes determining whether the key pair material is bound to a specific computer based on the tag data to meet the claim language).

According, Abgrall in view of Bernsteinet teaches:

(b) determining whether the key pair material is bound to the embedded security chip based on the tag data.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bernsteinet within the system of Abgrall because Bernsteinet teaches providing a cost effective before-the-fact digital media security system that is effectively transparent to the user / consumer, and minimally invasive and intrusive upon their privacy (Bernsteinet: Para [0001]).

6. Claims 1 – 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Abgrall et al. (U.S. Patent 2003/0037237), in view of Ansell (Patent Number 6792113).

As per claim 1, 7 and 16, Abgrall teaches a method for control of key pair usage in a computer system, the method comprising:

(a) creating key pair material for utilization with an embedded security chip of the computer system (Abgrall: Para [0191], [0105] and [0004] Line 16 – 19).

Abgrall teaches the key pair material is stored and bound to the embedded security chip. However, Abgrall does not disclose expressly the key pair material including tag data; and (b) determining whether the key pair material is bound to the embedded security chip based on the tag data.

Ansell teaches the key pair material including tag data (Ansell: Column 2 Line 49 – 53 and Column 2 Line 54 – 59: Examiner notes key pair material is made with a reasonable and broadest interpretations and referred to as “any crypto-key related information as a whole that enables the encryption / decryption functions” and Ansell discloses “hardware ID” as part of the machine-binding passport data structure – i.e. key pair material (Ansell: Column 2 Line 49 – 53) that is interpreted as the “tag data” to meet the claim language).

determining whether the key pair material is bound to a specific computer based on the tag data (Ansell: Column 2 Line 49 – 53 and Column 2 Line 54 – 59: Ansell discloses the tag data of either hardware-ID or user-password indicates, respectively, either a machine-binding or a user-binding is required and as such based upon the tag

data a machine-binding or a user-binding can be determined to meet the claim language).

According, Abgrall in view of Ansell teaches:

(b) determining whether the key pair material is bound to the embedded security chip based on the tag data.

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ansell within the system of Abgrall because Ansell teaches providing an enhanced security system that restricts unauthorized access to digital data and, in particular, for limiting access to such digital data only to either a particular machine or a particular user (Ansell: Column 1 Line 6 – 12).

As per claim 2, 9 and 17, Abgrall as modified teaches comprising a bit to indicate whether binding is required for the key pair material (Ansell: Column 2 Line 49 – 53 and Column 2 Line 54 – 59: Examiner notes key pair material is made with a reasonable and broadest interpretations and referred to as “any crypto-key related information as a whole that enables the encryption / decryption functions” and Ansell discloses the tag data of either hardware-ID or user-password indicates, respectively, either a machine-binding or a user-binding is required).

As per claim 3 and 11, Abgrall as modified teaches creating key pair material further comprises creating key pair material of different levels (Ansell: Figure 3A & 3B:

the four levels are (a) hardware ID key pair in the machine-binding passport data structure (Figure 3B Element 140) is qualified as a hardware key pair level) (b) machine-binding private key in the machine-binding passport data structure (Figure 3B Element 304) is qualified as a platform key pair level (c) user private key in the user-binding passport data structure (Figure 3A Element 304) is qualified as user key pair level and (d) content master key (i.e. application key) is qualified as a credential key pair level).

As per claim 4, 5, 12 and 13, Abgrall as modified teaches the four levels further comprise a hardware key pair level, a platform key pair level, a user key pair level, and a credential key pair level (Ansell: see for example, Figure 3A & 3B: the four levels are (a) hardware ID key pair in the machine-binding passport data structure (Figure 3B Element 140) is qualified as a hardware key pair level) (b) machine-binding private key in the machine-binding passport data structure (Figure 3B Element 304) is qualified as a platform key pair level (c) user private key in the user-binding passport data structure (Figure 3A Element 304) is qualified as user key pair level and (d) content master key (i.e. application key) is qualified as a credential key pair level).

As per claim 6 and 14, Abgrall as modified teaches tag data further comprises including a tag for indicating binding is required for the platform key pair level (Ansell: Column 2 Line 49 – 53 and Column 2 Line 54 – 59: Ansell discloses the tag data of either hardware-ID or user-password indicates, respectively, either a machine-binding

or a user-binding is required and as such based upon the tag data a machine-binding or a user-binding can be determined).

As per claim 8, Abgrall as modified teaches comprising means for security setup to provide an interface on the computer system for administration of the security processor, including providing the tag data (Ansell: Column 6 Line 16 – 18).

As per claim 10, Abgrall as modified teaches the security processor includes memory for storing the key pair material (Abgrall: [0004] Line 16 – 19).

As per claim 15, 18 and 19, Abgrall as modified teaches the key pair material further comprises a tag to indicate binding is not required for the user key pair level (Ansell discloses the tag data of either hardware-ID or user-password indicates, respectively, either a machine-binding or a user-binding is required and as such based upon the tag data, a machine-binding is not required can thus be determined if the tag data is a user-password – instead of a HW ID).

As per claim 20, 21 and 22, Abgrall as modified teaches the hierarchical structure is organized such that key pair material for portion of each of at least two levels of the hierarchical structure are not bound (Ansell: see for example, Figure 3A & 3B: the four levels are (a) hardware ID key pair in the machine-binding passport data structure (Figure 3B Element 140) is qualified as a hardware key pair level) (b) machine-binding

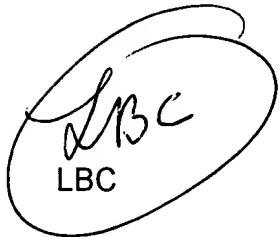
private key in the machine-binding passport data structure (Figure 3B Element 304) is qualified as a platform key pair level (c) user private key in the user-binding passport data structure (Figure 3A Element 304) is qualified as user key pair level and (d) content master key (i.e. application key) is qualified as a credential key pair level) – Therefore, Examiner notes the user private key level and content master level of the hierarchical structure are clearly not bound (i.e. at least two levels (c) & (d))

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



LBC

Longbit Chai  
Examiner  
Art Unit 2131

cel  
Primary Examiner  
AU2131  
12/16/05